NAVAL WAR COLLEGE
Newport, R.I.

INFORMATION WARFARE: EVALUATING INFORMATION TARGETS

by

Raymond Adamiec
LTCOL USMC

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature:

14 June 1996

Paper directed by
Col. G. Dillon

Faculty Advisor

Date

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED	
2. Security Classification Authority:	
3. Declassification/Downgrading Schedule:	
4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.	
5. Name of Performing Organization: Joint Military Operations Department	
6. Office Symbol: 1C	**7. Address:** Naval War College, 686 Cushing Rd., Newport, RI 02841-1207
8. Title (Include Security Classification): INFORMATION WARFARE: EVALUATING INFORMATION TARGETS (UNCLASSIFIED)	
9. Personal Author(s): Raymond Adamiec, Lieutenant Colonel, United States Marine Corps	
10.Type of Report: Final	**11. Date of Report:** 14 June 1996
12.Page Count: 25 including bibliography	
13.Supplementary Notation: A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.	
Ten key words that relate to your paper: Information warfare, information targets, target priority, organizational structure, defensive IW, offensive IW, deception, denial, destruction.	

15.Abstract: Information Warfare in its broadest definition has existed since armed conflict began. As the pace of battle accelerates and information collection intensifies it is necessary to have a means of synergistically combining the advanced technological tools, organizational structure and mathematical analysis of information target vulnerabilities. This essay provides a model to accomplish such a goal by establishing a framework to evaluate methods of employment, types of attack and desired results when prioritizing information targets.

16.Distribution / Availability of Abstract: UNLIMITED	**Unclassified** X	**Same As Rpt**	**DTIC Users**
18.Abstract Security Classification: UNCLASSIFIED			
19.Name of Responsible Individual: Chairman, Joint Military Operations Department			
20.Telephone: (401) 841-[redacted] 6461		**21.Office Symbol:** 1C	

INFORMATION WARFARE:

EVALUATING INFORMATION TARGETS

INTRODUCTION

Knowledge is Power[1]. Information Warfare (IW) in its broadest definition has existed since armed conflict began. Throughout history when a combatant knew more about his enemy's strengths and weaknesses, he had the necessary conditions for victory. When the combatant could then convert that knowledge into a capability, he generated sufficient conditions for victory. The conversion of knowledge to capability is the essence of information warfare.[2]

In past conflicts IW consisted of propaganda, psychological operations (PSYOPS), deception and Command and Control Warfare (C^2W). Today IW has moved beyond these rudimentary techniques and seeks to establish victory without war as a goal. IW properly applied, provides the capability to achieve that goal.

Although some may argue against the likelihood or feasibility of such warfare, one only need to recall that the attrition wars of the 20th century did not seem likely or feasible in the 17th or 18th century. Winning the wars of the future will require leaders to have the vision to choose appropriate information targets.

The model proposed in this essay will provide decision makers with a tool to attack IW targets effectively, with the proper degree of force, by synergistically combining IW technology, organizational structure and mathematical rigor.

DIFFICULTIES OF INTEGRATING IW TECHNIQUES

As combatant commanders attempt to integrate IW techniques into their arsenal, they face the same challenges that commanders faced when artillery, machine guns and tanks were first introduced onto the battlefield. They suddenly possessed new technology that provided significant potential without the tactics or doctrine to employ them. The successful commanders of the past were those who were able to integrate those weapon systems and employ them to achieve desired results.

Commanders who thoughtfully apply well-understood IW techniques, and do not indiscriminately use technological novelties, will gain victory on future battlefields.[3] Today's commanders must establish a clear methodology to integrate IW techniques into daily planning if they are to achieve victory.

AVAILABLE TOOLS

A report prepared by Science Applications International Corporation (SAIC) proposes an organizational structure to provide support to the Joint Command and Control Warfare Commander (JC^2WC). The JC^2WC when implemented, would be part of the J-3 and would provide the required coordination among the Intelligence (J-2), Operations (J-3) and Communications (J-6) Departments to evaluate IW targets.[4] These staffs require teamwork to meet the report's recommendations for a coordinated

way to conduct critical node analysis about friendly and enemy:

- command, control, communication, computers and intelligence (C^4I) nodes
- operational security (OPSEC) planning
- deception and counter-deception planning
- PSYOPS
- electronic warfare (EW)
- electronic attack
- electronic protection
- destruction and overall C^2W planning

The report provides a strong organizational foundation that assigns staff responsibilities, principal interfaces and recommends input and output data elements for each of the critical nodes listed above. The report does not provide the mathematical algorithms to convert input data elements to output values. In contrast, the Center for Naval Analysis (CNA) in a classified report has developed a method for quantifying the value of IW targets in military operations.[5] The methodology is mathematically sound and can easily be generalized to include more realistic scenarios and models.

THE MISSING PIECE

The commander now has an advanced IW technology, the SAIC-proposed structure for coordinating analysis of IW, and the CNA mathematical algorithms for evaluating specific actions in

specific scenarios. What is missing is a methodology that synergistically combines those three elements and provides decision makers with a quantifiable starting point to prioritize IW targets. The model adopted to perform this function should not be viewed as a substitute for the decision maker. Rather, it is a framework that uses a combination of mathematics and the opinions of technical analysts to extend the decision maker's judgment in making choices.

Such a model must be transparent. Transparency implies that the decision maker can understand and use the model as an extension of his or her own judgment. All assumptions are clearly described and held to manageable levels, and the deductive process leading to assertions is clear. Appraisal of the model also is necessary to assure the decision maker that the model is mathematically correct and uses valid data. Finally the model needs to be consistent to ensure that selection and evaluation of targets are analyzed in the same context and that the discussion of differing viewpoints is based on specific assumptions.

THE PROPOSED MODEL

A model to accomplish this analysis of IW targets would require three dimensions; a method of employment (offensive, defensive and manipulative), a type of attack (destruction, denial and deception) and a desired result (hard kills (H_k), soft kills (S_K) and exploitation). The proposed model should also

possess the capability to compare all combinations of each of the elements of these dimensions.

EMPLOYMENT METHODS

The employment methods of IW are offensive, defensive and manipulative. All three methods of employment are useful, if not necessary, throughout a campaign or major operation.

Offensive IW. The offensive category of IW is the heart of an IW campaign. The purpose of offensive action is the means by which a military force seizes and holds the initiative while maintaining freedom of action and achieving decisive results.[6] Offensive actions administer hard kills, soft kills and exploit enemy weaknesses to achieve strategic and operational objectives. Examples of offensive IW weapons include:

- Logic Weapons -- viruses, Electro- Magnetic Pulse (EMP) bombs, flaws, trap doors, RF weapons, data manipulation, covert channels, etc.[7]
- Conventional Weapons -- rifles and bombs.[8]

Defensive IW. Continuing the metaphor, if offensive IW is the heart of an IW campaign, defensive IW is what keeps the arteries to the heart clear. Defensive IW requires hardening, redundancy, protection and information denial. It is a doctrine of war not to assume the enemy will not come, but rather to rely on one's readiness to meet him; not to presume that he will not attack, but rather to make one's self invincible.[9] Defensive IW

aids this preparation. The best defensive IW measures are redundancy ~~and~~ deception.

Manipulative. Manipulation is the brains of IW. It is the skillful means of dealing with an adversary by altering his perception in a way that puts him at a distinct disadvantage. Manipulation profoundly affects information systems and, therefore, the knowledge available to make decisions. An example of manipulation is the use of non-cooperating "weapons". These weapons include technological systems used for IW purposes which, in some instances, occur without the owners' knowledge. The use of CNN during Desert Shield and Desert Storm is an example of a non-cooperative weapon.[10] Positioning is what the Madison Avenue advertising community uses to make people buy certain products. These techniques encourage or discourage certain behaviors.[11] Public Relations is the art of manipulation that is well understood in politics, marketing and publicity as a way to get people to think favorably about the subject of the pitch.[12]

TYPES OF ATTACK

Types of attack include, destruction, denial and deception. The value of each of these is dependent on the target, its vulnerability and the desired outcome of the attack.

Destruction. In most cases destruction is the easiest type of attack to execute. The goal of physical destruction is to damage the target in such a manner that it prevents the enemy

from using or rebuilding the target. Although this may be the easiest type of attack to perform, it may not be the most effective. In some cases it may be better not to destroy a target, for example, a telecommunications system, that the United States can use during post hostilities.

Denial. Denial prevents the enemy from using systems or sensors without destruction. Denial ranges from isolating systems to temporarily disabling them at critical times. Denial is a riskier type of attack than destruction, yet it can be extremely beneficial when conflict terminates and the attacked systems are required to attain the desired end state. Denial can be either covert or overt. Covert denial of services and corruption is more difficult for the enemy to detect than overt denial. For example, a virus that randomly substitutes one digit in spare parts requisitions can result in wrong items being sent and cause extreme difficulty for the requester to detect the source of the error. Most likely the requester will accept the errors as normal data entry problems. Slowly increasing the number of errors can deny the enemy a reliable logistics system.[13]

Deception. "All warfare is based on deception."[14] The object of deception is to deny an opponent knowledge of one's intentions and capabilities, actual or potential, and to provide him with counterfeit knowledge in as convincing a manner as possible.[15] For deception to be effective the enemy has to do three things, observe the deception, analyze the deception as

reality and act upon the deception according to the deceiver's goals. As systems increasingly remove the man in the loop, the deception can take place without the enemy observing or interpreting it. The system will automatically act on information inserted into it.[16] Another example of a deception technique is the Iraqi forces' successful employment of weapon mock-ups made from synthetic materials, coated with metallized paint and containing thermal emitters. These dummy targets on Iraqi territory received repeated attacks by coalition aircraft.[17]

DESIRED RESULTS

Throughout a campaign all actions should contribute to the desired end state. The execution of IW techniques is particularly important in this regard. The desired result of an IW attack falls into three categories, hard kill, soft kill and exploitation.

Hard Kill. A hard kill destroys or permanently disables the enemy's IW capabilities. Weapons used to achieve hard kills inflict physical damage on a target. Examples of hard kill weapons include high explosives, Electro-Magnetic Pulses, and High Power Microwaves (HPM).

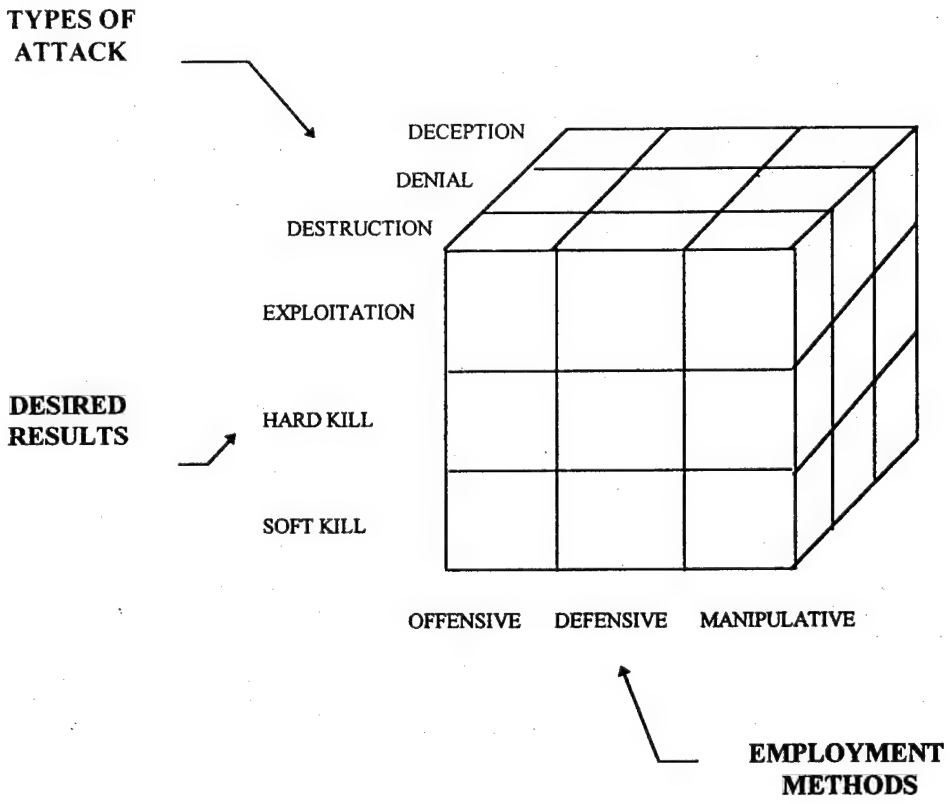
Soft Kill. Soft kills degrade a system. Examples of soft kill weapons that degrade the enemy's IW capabilities are delaying information, creating confusion, jamming, conditioning and misrouting information.[18] Delaying, misrouting, and jamming

are self explanatory. Conditioning is a slow introduction of errors into a system so that enemy operators of the system learn to tolerate the degradation as normal deficiencies, much as one becomes conditioned to cold temperatures over the course of a long winter. Confusion is the ability to randomly introduce and remove errors so that the enemy is unsure of what is a valid output.

Exploitation. Exploitation usually requires covert attacks against the enemy's IW targets. Exploitation of systems, including the media, is an area that can affect civilian leadership by influencing decisions. An effective campaign can achieve one of the goals of IW, i.e., defeating the enemy before battle begins. This is achieved by convincing the enemy, using his own systems for analysis, that hostile acts are futile. Another method of exploitation is saturation of the enemy's IW collection and processing systems. Overloading an information system with redundant and extraneous data has long been a vulnerability of hierarchical structures for command and control. By overwhelming an enemy's systems by perpetually generating data, an attacker seeks either to slow down legitimate computer operations, incapacitate the network through gridlock, or to cause the human receiving the avalanche of output to become ineffective.[19]

THE METHODOLOGY

The figure below provides a framework of the three dimensions of IW, employment methods, types of attack, and desired results.



The intent of the model is to aid the decision maker's judgment in IW target selection when used with the organizational structure recommended by SAIC and an expansion of the CNA algorithms.

THE PROCESS

Steps Required

1. Assign teams of IW technical analysts and operations research analysts to the JC²WC within the J-3.
2. JC²WC develops a set of targets or a target category.
3. Based on the CINC's guidance and J3 plans the JC²WC determines attack category (offensive, defensive, manipulative) type of attack (H_k, S_k, exploitative) and desired outcome (destruction, denial, deception).
4. Using the CNA study as a guide the operations research analysts formulate algorithms to calculate target value.
5. Include only the targets pre-approved by the decision maker.
6. Technical analysts review output for inconsistencies and errors (sanity check).

DETAILED INSTRUCTIONS FOR EACH STEP

STEP 1

Establish an appropriate team to build a valid working model. Technical analysts from CIA, NSA and DIA can provide current estimates of IW capabilities of potential enemies. The decision maker (CINC) must bound the options and target categories to remain within the scope of the assigned mission. He can do this in this step or step 5. A disadvantage of bounding the problem early in the process is that such a decision would possibly prevent the team discovering potential high value

targets. The advantage to early bounding of areas to explore allows a more focused approach. The team also requires operation research analysts to develop an algorithm with proper weighting of variables. The basic function would be:

$V_t = f(C_i\ A_j\ D_k)$

where V_t is the value of target t.
C_i is the method of employment (defense, offense, manipulative).
A_j is the type of attack (destruction, denial, deception)
D_k is the desired outcome (H_k, S_k exploitative)

The JC²WC can aid in establishing measures and weighting factors for targets.

STEP 2

Taking the target categories approved by the CINC, the JC²WC and subject matter experts can develop specific target sets. The four target categories available for the CINC to choose are, civilian leadership, civilian infrastructure, military leadership and military infrastructure. The annex explains these categories in greater detail.

STEP 3

The JC²WC and technical experts can determine the likelihood of a target being attacked and develop probabilities of success and failure. Consideration of each method of employment (offensive, defensive and manipulative) is necessary. Each type of attack (destruction, denial, deception) must then be compared

to the method of employment. Finally the desired outcome (H_k, S_k and exploitation) of the attack must be weighed against the target category and type of attack.

The following provides an example to aid in understanding the process: for a target category, develop target sets, and for each target in the set determine the values for C_i, A_j and D_k.

Example:

Target Category = Military infrastructure in theater.

Target Set = logistics systems, communication systems, etc.

Using the logistics system target (targets can be further refined to a specific logistics computer if desired), assign values for each method of employment of IW action.

C_1 = Offensive action against logistics system

C_2 = Defensive action for logistics system

C_3 = Manipulative action for logistics system

Values for type of attack

D_1 = Destruction of logistics system

D_2 = Denial of logistics system

D_3 = Deception of logistics system

Values for desired outcome of attack

A_1 = Hard kill against logistics system

A_2 = Soft kill against logistics system

A_3 = Exploitation attack against logistics system

The values assigned may be multidimensional, scaled values

or probabilities. An operations research analyst is required to formulate the appropriate measures.

STEP 4

The operations research analyst must then use the values in step 3 to develop a function, $f(C_iA_jD_k)$, to determine an overall target value. The basic formula is:

$V_t = f(C_i\ A_j\ D_k)$

Again for illustrative purposes only, the following is an example of how to use the values attained from step 3 to determine target values.

$f(C_1\ A_1D_1) = x_1$ .... $f(C_3A_1D_1) = x_{19}$

$f(C_1\ A_2\ D_1) = x_2$ ....

⋮

$f(C_1A_3D_3) = x_9$ .... $f(C_3A_3D_3) = x_{27}$

Summing x_1 to x_{27} will produce the value for a particular target. The x_n with the highest value is also the most effective combination against that target.

STEP 5

When the CINC allows an unbounded target set in step 1, he must then review the results and select target sets that are most appropriate for the assigned mission.

STEP 6

This is the sanity check step. Have technical experts review the results from the model. Inconsistent or wrong results require correction to the model, assignment of new values or development of alternative functions.

SUMMARY

In his theory of war Clausewitz emphasized the importance of converting knowledge into capability. With the compression of time and space in the modern world the importance of this conversion increases in value. Today's decision makers must convert knowledge to capability faster than the opponent. To make this conversion the decision makers need the latest technology, an organizational structure and realistic mathematical forecasting algorithms. More importantly they need a method to combine those ingredients in a transparent, appraised and consistent manner. Implementing the methodology proposed above will provide the decision makers with a significant advantage over their opponents in converting knowledge to capability, and thus winning the IW campaigns of the future.

ANNEX

TARGET SETS

CIVILIAN LEADERSHIP

Attacks on civilian leadership are attacks that disrupt the decision cycle for the executive, legislative and judicial branches. The more sophisticated a country is, the more sophisticated the attacker must be to achieve success that would have a direct effect on civil leadership.

CIVILIAN INFRASTRUCTURE

Throughout the public infrastructure computer viruses specially designed for use as a weapon might easily bring a modern computer dependent nation to its knees.[20]

Information Infrastructure: Computers, networks and media are self evident targets for IW.

Industrial Base: Production lines, research and development efforts and employment associated with the industrial base are potential high value targets.

Public Infrastructure: Elements of public infrastructure such as libraries, and local databases are lucrative targets.

Public Transit: The classic lines of communication are computerized in modern societies. Cutting these dilutes or denies the opponent's ability to move and creates chaos in the system.

Economy: The economy is vulnerable in a variety of ways including the financial support infrastructure (money transfer system).

MILITARY LEADERSHIP

Command and Control Infrastructure: The physical part of a Command and Control infrastructure includes microwave antenna, switching stations, telephone, radio, and modems. Non-physical is data, electrical systems, and support systems.[21]

MILITARY INFRASTRUCTURE

Autonomous Sensor System: Sensors that are designed to operate autonomously can be exploited to send false data back to a controlling system.[22]

C2 Infrastructure: Infrastructure includes the civilian and strategic leadership, the decision process, and societal support structures. Attacking these can sow discord, thereby fracturing the decision making process.[23]

Logistics: Modern logistics systems depend to a high degree on a computerized backbone that identifies supply requirements, positions material, tracks deliveries and schedules resources. Attacks on this system can severely affect the ability of forces to deploy.[24]

Integrated Air Defense: C^4I, TV, radio, telephone, fire control computers, strategic computer systems that identify missile launches and provide intelligence are lucrative targets.

NOTES

[1]Meditationes Sacrae [1597] De Haeresibus.

[2]J. Arquilla, "The Strategic Implications of Information Dominance," Strategic Review, Summer 1994, 25.

[3]David Carlton Controlling the International Transfer of Weaponry and Related Technology (Ipswich, Suffolk, Great Britain: Ipswich Book Co. 1995), 15.

[4]C. Wahl, and S. Hearold, Joint Command And Control Warfare Commander (JC2WC) Information And Display Requirements, Report 1680 (San Diego, CA: Naval Command, Control and Ocean Surveillance Center, August 1994), 3-4.

[5]Lloyd W. Koenig, An Approach To Quantifying The Operational Effectiveness Of Information Warfare - Main text (Alexandria, VA: Center for Naval Analysis, July 1994), 1-5.

[6]Joint Pub 3-0 Doctrine for Joint Operations A-1.

[7]Julie Ryan and Gary Federici. Offensive Information Warfare--A Concept Exploration (Alexandria, VA: Center for Naval Analysis, July 1994), 6.

[8]Ibid., 7

[9]Sun Tzu, The Art of War (Oxford: Oxford University Press, 1963), 114.

[10]Julie Ryan and Gary Federici. Offensive Information Warfare--A Concept Exploration (Alexandria, VA: Center for Naval Analysis, July 1994), 8.

[11]Ibid.

[12]Ibid.

[13]U.S. Defense Information Systems Agency, Planning Considerations for Defensive Information Warfare, Contract # DCA 100-90-C-0058 (Washington: 16 December 1993), 4.

[14]Sun Tzu, The Art of War (Oxford: Oxford University Press, 1963), 82.

[15] R.V. Jones, Future Conflict & New Technology (Beverly Hills, California: Sage Publications, 1981), 77.

[16] Cornerstones of Information Warfare, Pamphlet signed by the Secretary of the Air Force, 1995, 4.

[17] Mary C. Fitzgerald, The Impact of the Military-technical Revolutions on Russian Military Affairs, Contract # MDA903-91-C-0190 (Hudson Institute: August 1993), 24.

[18] J.R. Batzler and G.A. Federici Science and Technology Initiatives: Information Warfare, (Alexandria, VA: Center for Naval Analysis, February 1994), 13.

[19] S. Eisen, "Netwar, It's Not Just for Hackers Anymore," Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1995, 10.

[20] P. Evancoe, and M. Bentley. "CVW--Computer Virus as a Weapon." Military Technology, May 1994, 38.

[21] Julie Ryan and Gary Federici. Offensive Information Warfare--A Concept Exploration, (Alexandria, VA: Center for Naval Analysis, July 1994), 12.

[22] Ibid.

[23] Ibid.

[24] Ibid., 13

BIBLIOGRAPHY

Arquilla, J. "The Strategic Implications of Information Dominance." Strategic Review, Summer 1994, 24-30.

_____ and P.K. Davis. Thinking About Opponent Behavior in Crisis and Conflict: A Generic Model for Analysis and Group Discussion. Contract # MDA903-90-C-0004 Santa Monica: 1991.

_____ and D. Ronfeldt. "Cyberwar is Coming!" Comparative Strategy, April-June 1993, 141-165.

Arnett, Eric H. "Welcome to HYPER WAR." The Bulletin of the Atomic Scientists, September 1992, 14-18.

Batzler, J.R. and Federici, G.A. Science & Technology Initiatives: Information Warfare. Center for Naval Analyses: CAB 93-29, February 1994.

Busey, James B. "Information Security Dashes Thorny Power Projection Issues." Signal, November 1994, 13.

_____. "Information Warfare Calculus Mandates Protection." Signal, October 1994, 15.

Carlton, David, Klaus Gottstein, Elena Mirco, Paul Ingram, eds. Controlling the International Transfer of Weaponry and Related Technology. Ipswich, Suffolk, Great Britain: Ipswitch Book Co., 1995.

Cetron, Marvin J. "The Future Face of Terrorism." Futurist, November-December 1994, 10-14.

Clausewitz, Carl von. On War. Middlesex, England: Penguin, 1832.

Cornerstones of Information Warfare. Pamphlet signed by the Secretary of the Air Force, 1995.

Eisen, S. "Netwar, It's Not Just for Hackers Anymore." Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1995.

Evancoe, P. and M. Bentley. "CVW--Computer Virus as a Weapon." Military Technology, May 1994, 38-40.

Fitzgerald, Mary C. The Impact of the Military-Technical Revolutions on Russian Military Affairs. Contract # MDA903-91-C-0190, Hudson Institute: August 1993.

Fracker, M.L. "Conquest & Cohesion" in Challenge & Response, ed. K.P. Magyar. Alabama: Air University Press, 1994.

Grier, Peter. "The Data Weapon." Government Executive, June 1992, 20-23.

Grinter, Lawrence E. and Barry R. Schneider, eds. Battlefield of the Future. Maxwell AFB, Alabama: Air University Press, September 1995.

"Information Dominance Edges Toward New Conflict Frontier." Signal, August 1994, 37-40.

Jensen, O.E. "Information Warfare: Principles of Third-Wave War." Airpower Journal, Winter 1994, 35-43.

Jones, R.V. Future Conflict & New Technology. Beverly Hills, California: Sage Publications, 1981.

Kessel, R.M. "Parallel Warfare" in Challenge & Response, ed. K.P. Magyar. Alabama: Air University Press, 1994.

Klotz, Karlhorst. "Furtively Infecting the Enemy's Mainframe with an Equally Furtive Sickness." The German Tribune, 10 February 1991, 8.

Koenig, Lloyd W. An Approach To Quantifying The Operational Effectiveness Of Information Warfare - Main Text . Alexandria, VA: Center for Naval Analysis, July 1994.

Leibstone, Marvin. "U.S. Unmanned Air Vehicles." Military Technology, September 1992, 29-31.

Levy, Steven. "The Case for Hackers." Newsweek, 6 February 1995, 39.

Libicki, Martin C. "What is Information Warfare?" Strategic Forum, National Defense University, May 1995.

Lomov, N.A. The Revolution in Military Affairs (A Soviet View). Moscow: 1973.

Macedonia, M.R. "Information Technology in Desert Storm." Military Review, October 1992, 34-41.

McIntyre, John J., ed. The Future of Conflict. Washington DC: National Defense University Press, 1979.

Meyer, Michael. "Stop! Cyberthief!" Newsweek, 6 February 1995, 36-38.

Petersen, J.H. "Info Wars." U.S. Naval Proceedings, May 1993, 85-92.

Robinson, C.A., Jr. "Defense Organization Safeguards War Fighters' Information Flow." Signal, October 1995, 15-18.

Rogers, Adam. "A Borderless Dispute." Newsweek, 20 February 1995, 12.

Rowe, Wayne. "Information Warfare: A Primer for Navy Personnel." Unpublished Research Paper, U.S. Naval War College, Newport, RI: June 1995.

Ryan, Julie and Gary Federici. Offensive Information Warfare--A Concept Exploration. Alexandria, VA: Center for Naval Analysis, July 1994.

_____ Gary Federici and Tom Thorley. Information Support to Military Operations in the year 2000 and Beyond: Security Implications. Alexandria, Va: Center for Naval Analysis, July 1994.

Toffler, Alvin and Heidi Toffler, War and Anti-War. Boston: Little, Brown and Company, 1993.

Tzu, Sun. The Art of War. Oxford: Oxford University Press, 1963.

U.S. Defense Information Systems Agency. Planning Considerations for Defensive Information Warfare. Contract # DCA 100-90-C-0058. Washington: 16 December 1993.

U.S. Defense Intelligence Agency. The Intelligence Threat to DOD Computer Systems and Online Data Bases and Networks. DIW-2400-722-92. Washington: October 1992.

U.S. Joint Chiefs of Staff. Doctrine for Joint Operations. Joint Pub 3-0. Washington, D.C.: 1 February 1995.

_____. Doctrine for Joint Psychological Operations. Joint Publication 3-53. Washington, D.C.: 30 July 1993.

Wahl, C. and Hearold, S. Joint Command And Control Warfare Commander (JC2WC) Information And Display Requirements, Report 1680 San Diego, CA: Naval Command, Control and Ocean Surveillance Center, August 1994.

Wallich, Paul. "A Rogues Routing." Scientific America, May 1995, 31.